

# PathCanonicalize

The destination string buffer must be long enough to hold the return file path

Sean Barnum, Cigital, Inc. [vita<sup>1</sup>]

Copyright © 2007 Cigital, Inc.

2007-04-02

## Part "Original Cigital Coding Rule in XML"

Mime-type: text/xml, size: 4062 bytes

Attack Category	<ul style="list-style-type: none"><li>• Malicious Input</li><li>• Path spoofing or confusion problem</li></ul>		
Vulnerability Category	<ul style="list-style-type: none"><li>• Buffer Overflow</li></ul>		
Software Context	<ul style="list-style-type: none"><li>• File Path Management</li></ul>		
Location	<ul style="list-style-type: none"><li>• shlwapi.h</li></ul>		
Description	<p>The output buffer for the PathCanonicalize() function must be large enough to hold the result.</p> <p>The PathCanonicalize() function removes "." and ".." elements from a path, creating a full path specification without the relative references. The returned path is guaranteed to be the same length or shorter than the original.</p>		
APIs	Function Name	Comments	
	PathCanonicalize		
	PathCanonicalizeA		
	PathCanonicalizeW		
Method of Attack	Attacker can cause a buffer overflow if the destination parameter is not at least as long as the source buffer.		
Exception Criteria			
Solutions	Solution Applicability	Solution Description	Solution Efficacy
		For safety, make sure the first parameter, lpszDst, which is the destination buffer, is at least as long as the source buffer. It is safest to always	

1. [http://buildsecurityin.us-cert.gov/bsi/about\\_us/authors/35-BSI.html](http://buildsecurityin.us-cert.gov/bsi/about_us/authors/35-BSI.html) (Barnum, Sean)

		specify a buffer size of MAX_PATH characters.	
<b>Signature Details</b>	BOOL PathCanonicalize( LPTSTR lpszDst, LPCTSTR lpszSrc );		
<b>Examples of Incorrect Code</b>	<pre>// Path destination buffer. TCHAR buffer_1[10]; // Note: buffer is too small LPTSTR lpStr1; lpStr1 = buffer_1;  // Path to be Canonicalized. TCHAR buffer_3[ ] = TEXT("A: \\element_1\\..\\element_2\\.\\ \\element_3"); LPCTSTR lpStr3; lpStr3 = buffer_3;  PathCanonicalize(lpStr1,lpStr3);</pre>		
<b>Examples of Corrected Code</b>	<pre>// Path destination buffer. TCHAR buffer_1[MAX_PATH]; // Note: buffer is large enough LPTSTR lpStr1; lpStr1 = buffer_1;  // Path to be Canonicalized. TCHAR buffer_3[ ] = TEXT("A: \\element_1\\..\\element_2\\.\\ \\element_3"); LPCTSTR lpStr3; lpStr3 = buffer_3;  PathCanonicalize(lpStr1,lpStr3);</pre>		
<b>Source Reference</b>	<ul style="list-style-type: none"> <li><a href="http://msdn.microsoft.com/library/default.asp?url=/library/en-us/shellcc/platform/shell/reference/shlwapi/path/pathcanonicalize.asp">http://msdn.microsoft.com/library/default.asp?url=/library/en-us/shellcc/platform/shell/reference/shlwapi/path/pathcanonicalize.asp</a><sup>2</sup></li> </ul>		
<b>Recommended Resource</b>			
<b>Discriminant Set</b>	<b>Operating System</b>	<ul style="list-style-type: none"> <li>Windows</li> </ul>	
	<b>Languages</b>	<ul style="list-style-type: none"> <li>C</li> <li>C++</li> </ul>	

## Cigital, Inc. Copyright

Copyright © Cigital, Inc. 2005-2007. Cigital retains copyrights to this material.

Permission to reproduce this document and to prepare derivative works from this document for internal use is granted, provided the copyright and “No Warranty” statements are included with all reproductions and derivative works.

For information regarding external or commercial use of copyrighted materials owned by Cigital, including information about “Fair Use,” contact Cigital at [copyright@cigital.com](mailto:copyright@cigital.com)<sup>1</sup>.

The Build Security In (BSI) portal is sponsored by the U.S. Department of Homeland Security (DHS), National Cyber Security Division. The Software Engineering Institute (SEI) develops and operates BSI. DHS funding supports the publishing of all site content.

---

1. <mailto:copyright@cigital.com>